Northwestern Journal of Technology and Intellectual Property

Volume 16 | Issue 4 Article 4

2019

HACKING: THE NAKED AGE CYBERCRIME, *CLAPPER* & STANDING, AND THE DEBATE BETWEEN STATE AND FEDERAL DATA BREACH NOTIFICATION LAWS

Nicholas Ronaldson
Northwestern University Pritzker School of Law

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

HACKING: THE NAKED AGE

CYBERCRIME, *CLAPPER* & STANDING, AND THE DEBATE BETWEEN STATE AND FEDERAL DATA BREACH NOTIFICATION LAWS

Nicholas Ronaldson

May 2019 VOL. 16, NO. 4

Volume 16, Number 4 (2019)
Northwestern Journal of Technology and Intellectual Property

HACKING: THE NAKED AGE
CYBERCRIME, *CLAPPER* & STANDING, AND THE DEBATE BETWEEN STATE AND FEDERAL DATA BREACH NOTIFICATION LAWS

Nicholas Ronaldson

> "When you say I don't care about the right to privacy because I have nothing to hide, that is no different than saying I don't care about freedom of speech because I have nothing to say or freedom of the press because I have nothing to write."[1]
>
> — Edward Snowden

INTRODUCTION

In 2016, the FBI reported that on average more than 4,000 ransomware attacks occurred every day.[2] An October 2017 Equifax breach exposed the sensitive personal information of nearly 146 million Americans[3]—almost half of the United States population.[4] To make matters worse, after the Equifax breach, the public was directed to a phishing

[1] Alan Rusbridger et al., *Edward Snowden: NSA Reform in the US is Only the Beginning*, GUARDIAN (May 22, 2015, 12:46 PM), https://www.theguardian.com/us-news/2015/may/22/edward-snowden-nsa-reform [https://perma.cc/278K-22CA]; Guido, *Edward Snowden about Privacy*, YOUTUBE (Aug. 16, 2015), https://www.youtube.com/watch?v=bpO3GeXTceM [https://perma.cc/Y5QQ-2QB4].

[2] DEP'T OF JUSTICE, HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE: INTERAGENCY TECHNICAL GUIDANCE DOCUMENT 2 (June 2016), https://www.justice.gov/criminal-ccips/file/872771/download [https://perma.cc/6GAZ-F442].

[3] Ron Lieber, *How to Protect Yourself After the Equifax Breach*, N.Y. TIMES (Oct. 16, 2017), https://www.nytimes.com/interactive/2017/your-money/equifax-data-breach-credit.html [https://perma.cc/5YZV-NDKQ].

[4] *U.S. and World Population Clock*, U.S. CENSUS BUREAU, https://www.census.gov/popclock/ (last visited Apr. 18, 2019).

website to "check" if personal information was stolen.[5] The internet is the new Wild West for any tech-savvy individual, and, in this modern age, there is no telling how far the tech-horizon reaches.

State data breach notification laws are not uniform.[6] There also is no uniform federal statute governing data breach notification.[7] However, a state-by-state method, as will be analyzed in this note, is the best method for providing notice to consumers.

After a company is hacked, resulting in a data breach incident, the company is often placed in a tough situation and must determine whether to provide notice, how to provide notice, and how to best mitigate liability. These issues, in turn, have a ripple effect on consumers. After a serious breach, consumers are often left with a myriad of questions and concerns. Indeed, even consumers who sue the breached company in class-action lawsuits soon discover that they cannot establish standing.

The legal issues that technology has opened in this area are staggering and uncertain. With daily hackings, companies stand to lose millions of dollars, intellectual property, as well as brand trust. Concurrently, customers stand to have identities and personal information stolen without legal recourse. The innocence of the internet has faded in this naked age where nothing is secure, nothing is protected, and nothing can be covered up.

This is a walk-through note that is organized into four sections. The first section is an explanation and background on various hacking methods. The second section is an overview of *Clapper v. Amnesty Int'l USA*.[8] The third section examines *Remijas v. Neiman Marcus Group, LLC*.[9] Finally, the fourth section is a two-part analysis that discusses the following: (1) how *Clapper* and *Remijas* work in harmony for determining consumer standing after a breach, and (2) the benefits that state data breach notification laws provide, as opposed to a uniform federal notification standard.

---

[5] Merrit Kennedy, *After Massive Data Breach, Equifax Directed Customers to Fake Site*, NPR (Sept. 21, 2017, 5:13 PM), http://www.npr.org/sections/thetwo-way/2017/09/21/552681357/after-massive-data-breach-equifax-directed-customers-to-fake-site [https://perma.cc/D92S-63QK].

[6] *See* LIISA M. THOMAS, THOMAS ON DATA BREACH: A PRACTICAL GUIDE TO HANDLING DATA BREACH NOTIFICATIONS WORLDWIDE 3 (2017); *see also* Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 402 (2016).

[7] *See* Kathryn E. Picanso, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 389–90 (2006).

[8] Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).

[9] Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688 (7th Cir. 2015).

I. HOW DO HACKERS HACK?

The ways in which hackers hack into a company, database, or system are creative, secretive, and important to understand. This note will next discuss several of the common ways that hackers hack.[10]

First, "spear fishing," or email social engineering, is a very common tactic utilized by hackers.[11] Under this method, hackers send an email or an instant message directly to a target at a company.[12] Once the message is opened, malware is released and it then seeks any vulnerabilities in the system.[13] Once the malware is in the system a communication channel will open between the hacker and the system, allowing the hacker to control and browse the system.[14] Finally, once inside the system, the hacker can use the infected computer as a "beachhead" allowing access to other machines within the network.[15]

Infection via a "drive-by" web download is where a hacker implants a piece of code that infects any user who goes onto the website.[16] When the web-surfer visits, or "drives-by" the web-page, the malicious code gains access to the web-surfer's computer and begins to download in the background of the web-surfer's computer—unbeknownst to the web-

[10] Michelle Fox, *10 Ways Companies Get Hacked*, CNBC (July 6, 2012, 12:22 PM), https://www.cnbc.com/2012/07/06/10-Ways-Companies-Get-Hacked.html [https://perma.cc/97Q9-39TL483D-9W6G]. Hackers hack in a few of the following ways: "spear fishing"; infection via a "drive-by" web download; USB key malware; scanning networks for vulnerabilities and exploitation; guessing or social engineering passwords; Wi-Fi compromises; stealing credentials from third-party sites; compromising web-based databases; exploiting password reset services to hijack accounts; and through insider infiltration. *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.*; *see also* Margaret Rouse, *Malware (Malicious Software)*, TECHTARGET, http://searchsecurity.techtarget.com/definition/malware [https://perma.cc/WLV5-T2SX] ("Malware, or malicious software, is any program or file that is harmful to a computer user. Malware includes computer viruses, worms, Trojan horses and spyware. These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission.").

[14] Fox, *supra* note 10. This is why it is very important to be careful and cognizant of what you are clicking and opening while on the internet.

[15] *Id.*; *see also* April Glaser, *A Massive Google Docs Hack Is Spreading Like Wildfire*, RECODE (May 3, 2017, 4:23 PM), https://www.recode.net/2017/5/3/15535018/google-docs-hack-spreading-email-phishing [https://perma.cc/GJ2Z-PD8X] ("When you click on the link to open the file, you are directed to grant access to an app that looks like Google Docs but is actually a program that sends spam emails to everyone you've emailed. . . . The practice of sending an email in order to trick someone into granting access to their personal information is called phishing, and it's usually done for malicious reasons, like to steal credit card information or trick them into sharing their password.").

[16] Fox, *supra* note 10, at 3; *What is a "Drive-By" Download?* MCAFEE (Apr. 2, 2013), https://securingtomorrow.mcafee.com/consumer/family-safety/drive-by-download/ [https://perma.cc/33SW-CMBV] (this type of access can also occur through other types of devices, not strictly computers).

surfer.[17] Thus, the website appears innocent while the malicious code is being installed on the web-surfer's device.

Hackers scan networks for vulnerabilities using a point-of-entry exploitation method.[18] Under this method, hackers send commands to a server, attempt to crash the server, and then attempt to install malicious code on the crashed system.[19]

Hackers also guess or socially engineer passwords.[20] According to one survey, the three most common passwords in the world are "123456," "123456789," and "qwerty."[21] Socially engineering passwords is similar to "Facebook stalking."[22] Hackers research their target's various social media accounts to determine answers to password reset questions—which in turn can provide access to login information.[23] Hackers also directly contact

---

[17] Fox, *supra* note 10, at 5.

[18] *Id.* This point-of-entry exploitation method is particularly prevalent among smaller companies with weaker security systems.

[19] *Id.* There are even step-by-step tutorials to teach hackers how to conduct point-of-entry exploitations. *See* OCCUPYTHEWEB, *Hack Like A Pro: How to Scan for Vulnerabilities with Nessus,* WONDER HOW TO (Apr. 5, 2016, 11:00 AM), https://null-byte.wonderhowto.com/how-to/hack-like-pro-scan-for-vulnerabilities-with-nessus-0169971/ [https://perma.cc/72T3-XPF2].

[20] Fox, *supra* note 10, at 6.

[21] Shivali Best, *Will We Ever Learn? 123456 Is STILL the World's Most Popular Password: Here Are the Top 25 Phrases to Avoid*, DAILYMAIL (Jan. 16, 2017), http://www.dailymail.co.uk/sciencetech/article-4125128/The-common-passwords-used-2016.html#ixzz4yo3lblhZ [https://perma.cc/52WB-YC29]. Granted, this type of survey and result can easily be undermined because these "three most popular" may simply be the product of a minority of internet users. For instance, if all the world's population has wildly different and complicated passwords, but four people have "123456" as their password, three people have "123456789," and three people use "qwerty," now these three are the "world's most popular passwords." Cynicism aside, a study like this does go to show that most people have easy-to-guess-passwords that are overused and that do not provide enough protection from hackers.

[22] *Facebook Stalking*, TECHOPEDIA, https://www.techopedia.com/definition/27873/facebook-stalking [https://perma.cc/A3S9-STRE].

[23] Fox, *supra* note 10. This is where a hacker can use Facebook to determine basic information about their target that is often asked in security questions. *See also* Lily Hay Newman, *Time to Kill Security Questions—Or Answer Them With Lies*, WIRED (Sep. 28, 2016, 7:00 AM), https://www.wired.com/2016/09/time-kill-security-questions-answer-lies/ [https://perma.cc/NXS3-9BE8] ("The best way to make security answers more robust is to lie in your answers, and ideally use a random string of characters as the answer instead of submitting any meaningful information. That way, even if a question addresses an obscure life detail that you're confident a hacker couldn't find out about you, you're still not revealing answers that could be compromised in a breach."); Brandon Specktor, *Your Password Recovery Questions are Insanely Easy to Hack—and You Might Be to Blame*, READER'S DIGEST, https://www.rd.com/advice/work-career/password-recovery-questions/ [https://perma.cc/99EW-D524] (a hacker allegedly breached Mitt Romney's personal email by determining the name of Mitt's dog's name, which turned out to be the answer to Mitt's password reminder and reset). For instance, if a password reset security question is "What was the name of the street you grew up on?" or "What is your freshman year college roommate's name?" Google Maps and Facebook can likely provide the answer to a determined hacker. Thus, your childhood street name should probably be something like, "S7v]^be", and your college roommate's name should be, "jIf73)|(3,Nckidow093Jf0".

employees asking to reset their password, which provides the hacker the employee's password.[24]

Wi-Fi is another avenue for hackers to invade a system.[25] For instance, hackers can position themselves near or even inside a business's physical location—close enough to be in range of the Wi-Fi—and then engage in a series of different methods to find an unsecured or poorly secured system to steal information from.[26]

Hackers further obtain personal credentials by going through third-party websites, a method known as "collateral hacking."[27] For example, a hacker may go onto a website such as LinkedIn, find a target who works for a desired company, and proceed to hack the third-party website to steal the target's username and password.[28] People often use the same login information or slight variations of it for multiple websites.[29] Thus, if the hacker obtains the login information for one website, there is a high probability that they will be able to use that login information for other websites.[30]

---

[24] Fox, *supra* note 10, at 10; *see also* Sam Shead, *Hackers are Offering Apple Employees in Ireland up to €20,000 for Their Login Details*, BUSINESS INSIDER (Feb. 9, 2016, 6:49 AM), http://www.businessinsider.com/hackers-offering-apple-employees-in-ireland-euros-login-details-2016-2 [https://perma.cc/YH7D-KUU9].

[25] Fox, *supra* note 10, at 7.

[26] Philip Bates, *5 Ways Hackers Can Use Public Wi-Fi to Steal Your Identity*, MAKEUSEOF (Oct. 23, 2016), http://www.makeuseof.com/tag/5-ways-hackers-can-use-public-wi-fi-steal-identity/ [https://perma.cc/XZ5J-7T7K] (five ways hackers can use public Wi-Fi to steal information about you: (1) "Man-in-the-Middle Attacks," (2) Fake Wi-Fi Connections, (3) "Packet Sniffing" (4) "Sidejacking" (Session Hacking), and (5) "Shoulder-Surfing").

[27] Vangie Beal, *collateral hacking*, WEBOPEDIA, https://www.webopedia.com/TERM/C/collateral_hacking.html [https://perma.cc/HFW6-ULW9] ("Collateral hacking refers to when a company's critical data is compromised as a result of a third party in possession of the company's sensitive data being hacked. Rather than directly hacking into a company, collateral hackers go through a third party in order to get to the company's sensitive data. Collateral hacking frequently results in additional companies having their data compromised, as the third-party firm will often have the data of numerous companies stored on the hacked server or resource. The security concern of collateral hacking has become more prevalent with the increasing popularity of companies storing sensitive data via server virtualization, in the cloud or with other third-party storage hosting services.").

[28] Fox, *supra* note 10, at 8.

[29] Graham Cluley, *55% of Net Users Use the Same Password for Most, if Not All, Websites. When Will They Learn?* NAKED SECURITY: SOPHOS (Apr. 23, 2013), https://nakedsecurity.sophos.com/2013/04/23/users-same-password-most-websites/ [https://perma.cc/A5HW-969N] ("[A] poll of 1805 adults aged 16 and over discovered that 55% of them used the same password for most – if not all! – websites.").

[30] *Id.*; *see also Amazon.com's Third-Party Sellers Hit by Hackers*, FOX BUS. (Apr. 10, 2017), http://www.foxbusiness.com/markets/2017/04/10/amazon-coms-third-party-sellers-hit-by-hackers.html [https://perma.cc/6P6B-DZDK].

Finally, hackers infiltrate and access personal information through the use of code and web-based databases.[31] Information entered onto a website generally "gets stored in that company's database."[32] Hackers create malicious text (damaging code) that, when entered into the company database, stops the database from running its normal code; instead, the database runs the malicious text.[33] This "malicious takeover of the system"[34] often goes unnoticed due to the high volume of activity that regularly occurs on databases.[35]

The issue of hacking and data breaches is pervasive. There is a high probability that your information has already been taken. Understanding hacking leads to a better understanding of the personal, legal, and policy implications behind data breach incidents.

This note next addresses two foundational cases: *Clapper* and *Remijas*. During the discussion on *Clapper* and *Remijas*, the note then will turn into a discussion on how these two opinions formulate the proper analysis for determining standing for consumers after their information has been hacked in a data breach.

II. CLAPPER V. AMNESTY INTERNATIONAL

Clapper concerns the issue of standing under Article III of the Constitution.[36] This widely discussed case is important to analyze when considering the effects that a data breach incident can have on consumers' legal standing.

In *Clapper*, the respondents consisted of "attorneys and human rights, labor, legal, and media organizations."[37] The nature of the respondents' work required them to engage with clients located outside the United States via telephone and e-mail.[38] Respondents brought a constitutional

---

[31] Fox, *supra* note 10, at 9.

[32] *Id.*

[33] *See id.*

[34] *Id.*

[35] Kelly Jackson Higgins, *Hacker's Choice: Top Six Database Hacks*, UBM: DARK READING (May 8, 2008, 10:20 AM), https://www.darkreading.com/risk/hackers-choice-top-six-database-attacks/d/d-id/1129481? [https://perma.cc/G5PT-NB5J] (discussing that the average hacker needs only 10 seconds to hack in and out of a database, and, when coupled with the fact that a typical database has tens of thousands of connections per second, there can be virtually no way to know what these connections are really doing).

[36] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) ("To establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'") (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 140 (2010)).

[37] *Clapper*, 568 U.S. 398, 406.

[38] *Id.*

challenge[39] against § 702 of the Foreign Intelligence Surveillance Act of 1978 ("FISA").[40] They sought a declaration that § 1881a (where § 702 of FISA is codified) is unconstitutional, as well as an injunction against § 1881a-authorized surveillance.[41]

Respondents made several claims: (1) the government has targeted respondents' clients under FISA;[42] (2) the government believes respondents' clients are associated with terrorist organizations;[43] (3) for counterterrorism and diplomatic reasons, the government has focused on the locations where respondents' clients live; (4) the government believes that the respondents' clients oppose U.S.-backed governments;[44] and (5) that because of FISA, respondents are forced to take costly measures to avoid surveillance and to protect the confidentiality of their communications.[45]

Looking at the procedural posture, the government first prevailed at the district court.[46] However, the Second Circuit reversed and found for plaintiff-respondents,[47] but then denied a rehearing *en banc*.[48] The

---

[39] *Id.* at 401.

[40] 50 U.S.C. § 1881a (2012). FISA "allows the Attorney General and the Director of National Intelligence to acquire foreign intelligence information by jointly authorizing the surveillance of individuals who are not 'United States persons' and are reasonably believed to be located outside the United States." *Clapper*, 568 U.S. at 401 (quoting § 1881a). This section of FISA has generated an enormous amount of controversy, especially regarding warrantless searches of U.S. citizens. Under FISA, the government can collect communications of Americans who communicate with other Americans who communicate with targeted individuals. In other words, if A is the target, and A talks to B, and B talks to C, the government can collect C's communications because C talked to B who talked to A. *Decoding 702: What is Section 702?*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/702-spying [https://perma.cc/TE8S-25JB]. As Senator Rand Paul stated, "Millions of Americans are accidentally or incidentally collected in this database, and we don't want people just willy-nilly looking into this database without a warrant." Kaitlyn Schallhorn, *FISA Surveillance Program: What is It and Why is It So Controversial?,* FOX NEWS (Jan. 19, 2018), http://www.foxnews.com/politics/2018/01/19/fisa-surveillance-program-what-is-it-and-why-is-it-so-controversial.html [https://perma.cc/S85R-5GXH]. For an interesting discussion on the uncharted waters of computer searches, see Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 540 (2005) (discussing that "[t]he differences between homes and computers prompt an important question: what does it mean to 'search' a computer storage device?"); *see also In re* Search of Info. Associated With [Redacted]@mac.Com That Is Stored At Premises Controlled By Apple, Inc., 13 F. Supp. 3d 145, 147 (D.D.C. 2014) (discussing a government attempt to search and seize an entire email account); United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010) (discussing a warrantless search and seizure of thousands of emails with regards to the Stored Communications Act).

[41] *Clapper*, 568 U.S. at 401.

[42] *Id.* at 406.

[43] *Id*.

[44] *Id.*

[45] *See id.* at 405–406.

[46] Amnesty Int'l USA v. McConnell, 646 F. Supp. 2d 633, 635 (S.D.N.Y. 2009), *vacated* 638 F.3d 118 (2d Cir. 2011), *rev'd* 568 U.S. 398 (2013).

[47] Amnesty Int'l USA v. Clapper, 638 F.3d 118, 122 (2d Cir. 2011), *rev'd* 568 U.S. 398 (2013).

government appealed, and the United States Supreme Court granted certiorari.[49] In an opinion by Justice Alito, the Supreme Court reversed the Second Circuit, finding in favor of the government in a 5-4 decision.[50]

First, "[t]o establish Article III standing," respondents needed to establish that they suffered an injury that was "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[51] Justice Alito emphasized that the Supreme Court has "repeatedly reiterated that the 'threatened injury must be *certainly impending* to constitute injury in fact,' and that [mere] '[a]llegations of *possible* future injury' are not sufficient" to establish standing.[52] Justice Alito then addressed each of respondents' claims.

First, respondents failed to demonstrate the "imminent" requirement under Article III to establish standing.[53] Justice Alito noted that it is sheer speculation as to "whether the Government will imminently target communications to which *respondents* are parties."[54] Rather, "respondents' theory necessarily rests on their assertion that the Government will target *other individuals*—namely, their foreign contacts."[55] Additionally, respondents also failed to produce evidence demonstrating that their communications had, in fact, already been monitored.[56] In sum, Justice Alito dismissed all of respondents' claims that the government has or will target their communications as sheer conjecture.

Next, even if respondents could prove that government surveillance was imminent, they failed to show that "their injury is fairly traceable to § 1881a."[57] Simply put, the government has many means to conduct surveillance. Here, respondents' assertion that the government would do so under § 1881a, instead of a different authority, was deemed sheer

---

[48] Amnesty Int'l USA v. Clapper, 667 F.3d 163, 164 (2d Cir. 2011).

[49] Clapper v. Amnesty Int'l USA, 566 U.S. 1009 (2012).

[50] *See Clapper*, 133 568 U.S. 398, 422.

[51] *Id.* at 409. (quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010)).

[52] *Id.* (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)). The issue and holding in *Clapper*—whether respondents could establish Article III—are widely used by lower courts in data breach cases. Thus, the issue arises whether, when consumers' personal information (e.g. social security number, name, financial information, etc.) is stolen in a data breach, is that injury "concrete, particularized, and actual or imminent"? *See Clapper*, 568 U.S. 398 at 409. Is it "*certainly* impending to constitute injury in fact"? *See id.* Or are consumers merely alleging "possible future injury"? *See id.*

[53] *Clapper*, 568 U.S. 398 at 411.

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *Id.* at 412.

speculation. Thus, the Court held that respondents could not satisfy the fairly traceable requirement.[58]

Justice Alito next noted that even if respondents could prove the imminent and fairly traceable requirements, they "can only speculate as to whether [the Foreign Intelligence Surveillance Court of Review (FISC)] will authorize such surveillance."[59] Justice Alito stated, "In the past, we have been reluctant to endorse standing theories that require guesswork as to how independent decisionmakers will exercise their judgment."[60] Thus, respondents offered nothing but speculation as to how FISC will decide a government plan to surveil under § 1881a.

Fourth, Justice Alito explained that, even with FISC's approval, it is not clear that the government would actually be successful in their surveillance of respondents' clients.[61] Fifth, Justice Alito noted that "even if the Government were to conduct surveillance of respondents' foreign contacts, respondents can only speculate as to whether *their own communications* with their foreign contacts would be incidentally acquired."[62] In sum, respondents failed to offer anything other than speculation and conjecture in their attempt to establish standing.[63]

Respondents' alternative argument was that in attempting to avoid government surveillance under § 1881a, they suffered injury sufficient to establish standing.[64] Both arguments were summarily dismissed.[65] The Court held that respondents lacked Article III standing and reversed the Second Circuit.[66]

---

[58] *Id.*

[59] *Id.* at 412-414. Thus, even if the government was targeting respondents under § 1881a, the Foreign Intelligence Surveillance Court of Review (FISC) must first approve any government action to surveillance—respondents offered nothing but speculation on how FISC would rule. This is also important to keep in mind when lower courts use the holding in *Clapper* for determining standing after a data breach. Namely, there is no court acting as a gatekeeper determining which hackers have access to personal and financial information. In contrast, the government here bears the burden of proving their case to a court in the hope of being granted permission to attempt to surveil the desired target.

[60] *Id.* at 413.

[61] *Id* at 414.

[62] *Id.*

[63] *Id.* As Justice Alito states, "In sum, respondents' speculative chain of possibilities does not establish that injury based on potential future surveillance is certainly impending or is fairly traceable to § 1881a." *Id*.

[64] *Id.*

[65] Consider the following factual analogy to be drawn here compared with a data breach. Namely, that in *Clapper* respondents took measures to avoid future injury (but failed to establish standing because the injury was speculative). Whereas after a consumer's information is stolen in a data breach, they may seek costly credit monitoring and other preventative measures to protect against identity theft and fraud. The question of whether this establishes standing is next addressed in *Remijas* below.

[66] *Clapper*, 568 U.S. 398 at 422.

The dissent, written by Justice Breyer and joined by Justice Ginsburg, Justice Sotomayor, and Justice Kagan, focused on whether the injury (the interception of communication) was actual or imminent.[67] Justice Breyer did not view respondents' harm as speculative.[68]

III. *REMIJAS* AND *CLAPPER* IN THE DATA BREACH CONTEXT

The Seventh Circuit in *Remijas*[69] established a clear standard for determining standing in data breach lawsuits by distinguishing *Clapper*. After *Clapper*, many lower courts read its holding broadly and denied standing for those who had been affected in data breaches.[70] *Remijas* recognized the clear factual differences between issues of national security and that of commercial data breaches.[71]

In *Remijas*, approximately 350,000 credit cards had been exposed to malware on Neiman Marcus' system.[72] The cyberattack produced nearly 9,200 cards that were fraudulently used.[73] Plaintiffs, a group of affected customers, brought a class-action lawsuit.[74] Plaintiffs brought a variety of claims, including violation of multiple state data breach laws, totaling over $5,000,000 in damages.[75]

Neiman Marcus moved to dismiss for lack of standing and failure to state a claim.[76] The motion was granted by the district court based exclusively on standing.[77]

On appeal, the Seventh Circuit reversed and found standing for plaintiffs.[78] The court examined whether plaintiffs satisfied "*Clapper's*

---

[67] *Id.* at 424 (Breyer, J., dissenting).

[68] *Id* at 422. This note need not thoroughly address the dissent because, while persuasive and well-researched, it is not relevant to the topic of this note.

[69] Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 697 (7th Cir. 2015).

[70] *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017); Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 856 (S.D. Tex. 2015); Green v. eBay Inc., No.14 1688, 2015 WL 2066531, at *4 (E.D. La. May 4, 2015); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 24 (D.D.C. 2014); *In re* Barnes & Noble Pin Pad Litig., No. 12-CV-8617, 2013 WL 4759588, at *2 (N.D. Ill. Sept. 3, 2013), vacated *sub nom*. Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826 (7th Cir. 2018).

[71] *Remijas*, 794 F.3d at 693-94.

[72] *Id.* at 690.

[73] *Id.*; *see also* Evan Schuman, *Neiman Marcus Data Breach Settlement Tells Us Plenty About the ROI of Security: When Breaches Cost So Little, There's Not Much Incentive to Avoid Them*, COMPUTERWORLD: IDG COMMUNICATIONS (Apr. 3, 2017), [https://perma.cc/9W23-CJHB] (discussing the cost benefit analysis of notifying customers of the breach of their personal information).

[74] *Remijas*, 794 F.3d at 690.

[75] *Id.* at 690–91.

[76] *Id.* at 691. Neiman Marcus cited Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6).

[77] *Id.*

[78] *Id.* at 697.

requirement that [the] injury either already have occurred or be 'certainly impending.'"[79]

The court stated that plaintiffs "should not have to wait until hackers commit identity theft or credit-card fraud in order to [have] standing, because there is an 'objectively reasonable likelihood' that such an injury will occur."[80] Indeed, the court plainly stated that, "it is plausible to infer that the plaintiffs have shown a substantial risk of harm. . . . *Why else would hackers break into a store's data base and steal consumers' private information*?"[81] The court next clarified their position in light of the holding in *Clapper*, noting that *Clapper* does not prevent establishing standing based on future injuries.[82]

Finally, the court examined plaintiffs' allegation that they had lost time and money in taking protective measures against future harm (fraud and identity theft).[83] Judge Wood again distinguished *Clapper* and stated, "[o]nce again, however, it is important not to overread *Clapper*. *Clapper* was addressing speculative harm based on something that may not even have happened to some or all of the plaintiffs."[84] In distinction, Judge Wood noted that unlike the speculation in *Clapper*, the facts in *Remijas* clearly satisfy the issue of standing.[85] Simply put, Judge Wood stated, "[t]hat easily qualifies as a concrete injury."[86]

IV. ANALYSIS

This note will next address how these two opinions formulate the proper analysis for determining standing after a data breach incident.

---

[79] *Id.* at 692.

[80] *Id.* at 693.

[81] *Id.* (emphasis added).

[82] *Id.* Specifically, Judge Wood found key language in *Clapper*:

[*Clapper*] stated that "[o]ur cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about . . . . [W]e have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm."

Id. (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013)).

[83] *Id.* at 694.

[84] *Id.*

[85] *Id*. Judge Wood noted that it was not even contested by Neiman Marcus that a breach had occurred; that affected and notified customer might reasonably believe it necessary to receive monthly credit monitoring; that Neiman Marcus was in fact offering free credit monitoring for a year; and that credit-monitoring is not cheap. These helped in her determination that standing was proper. *Id.* For an interesting discussion on injury and harm see Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data -Breach Harms*, 96 TEX. L. REV. 737 (2018).

[86] *Remijas*, 794 F.3d at 694.

Finally, this note will discuss the benefit that state data breach notification laws provide, as opposed to a uniform federal notification law.

Courts have read *Clapper* in the overly broad light that *Remijas* counseled against with regards to data breach incidents and consumer standing in litigation.[87] Additionally, law review articles are critical of *Clapper* because of the uncertainty surrounding its holding—i.e., whether it "tightens" the requirements to establish standing after a data breach or whether it is merely a very narrowly written opinion.[88]

The criticism of *Clapper* and its ostensible "tightening" is misguided. *Clapper* does not create a tightening[89] on what is necessary for standing in

---

[87] *See In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 28 (D.D.C. 2014) (noting that "since *Clapper* was handed down last year, courts have been even more emphatic in rejecting 'increased risk' as a theory of standing in data-breach cases."); *In re* Barnes & Noble Pin Pad Litig., No. 12-CV-8617, 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013) (noting that "[m]erely alleging an increased risk of identity theft or fraud is insufficient to establish standing. *But see* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388–89 (6th Cir. 2016) (noting that "Plaintiffs' allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage of the litigation" and that "[t]his conclusion is in line with two recent decisions from the Seventh Circuit addressing standing in data-breach cases[,]" namely, *Remijas* and Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016)); *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014) (noting that "*Clapper's* discussion of standing arose in the sensitive context of a claim that other branches of government were violating the Constitution, and the U.S. Supreme Court itself noted that its standing analysis was unusually rigorous as a result.").

[88] *See, e.g.*, *Standing - Challenges to Government Surveillance - Clapper v. Amnesty International USA*, 127 HARV. L. REV. 298, 303 (2013) ("The *Clapper* majority does not make clear whether the 'certainly impending' standard applies to all future litigants of any kind, or only to those challenging governmental action in intelligence or foreign affairs."); John Biglow, *It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation*, 17 MINN. J. L. SCI. & TECH. 943, 955 (2016) ("In the wake of *Clapper*, it seemed unclear whether data breach cases in which plaintiffs lack actual misuse of data would be able to survive a *Clapper* challenge to standing."); Thomas Martecchini, *A Day in Court for Data Breach Plaintiffs: Preserving Standing Based on Increased Risk of Identity Theft After Clapper v. Amnesty International USA*, 114 MICH. L. REV. 1471, 1478–79 (2016) ("The Supreme Court's subsequent consideration of increased risk standing in a separate context—in *Clapper v. Amnesty International USA*—only compounded the uncertainty created by the circuit split."); Claire Wilka, *The Effects of Clapper v. Amnesty International USA: An Improper Tightening of the Requirement for Article III Standing in Medical Data Breach Litigation*, 49 CREIGHTON L. REV. 467, 471–75 (2016) (showing disparity among lower courts' interpretation of *Clapper*); *see also* James C. Chou, *Cybersecurity, Identity Theft, and Standing Law: A Framework for Data Breaches Using Substantial Risk in a Post-Clapper World*, 7 AM. U. NAT'L SEC. L. BRIEF 120, 181 (2017) (presenting a framework for standing in light of *Clapper*).

[89] In *Moyer*, the defendants argued that the United States Supreme Court in *Clapper* tightened the requirements for standing for injuries based on a future risk of harm. Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at*4 (N.D. Ill. July 14, 2014). The Moyer court disagreed. *Id.* at *5. There the court noted that the injury-in-fact requirement was applied so rigorously in *Clapper* because *Clapper* was addressing a much different issue: the constitutionality of a congressional law in light of a national security issue. *Id.* at *5-6. The issue in *Clapper* is not connected nor similar to a data security breach that involves the identity theft and the future possibility of harm. Also, *Clapper* was attenuated;

data breach lawsuits. The Seventh Circuit's decision in *Remijas*[90] clearly demonstrates that *Clapper* is factually distinct from data breach lawsuits.[91] Indeed, *Clapper* is very narrowly written and should be read accordingly.[92] Thus, *Clapper* must be read in light of the context in which it was written: national security. To simply cut and paste its Article III standing analysis based on speculative and future injury into any category that roughly fits is error. As such, *Clapper* and *Remijas*, read in tandem, are in harmony and provide a clear and workable standard for determining standing for post-data breach incidents.

This note now makes its final turn towards data breach notification laws. Looking back at how these events unfold, they first start with a hacking. Then there is a data breach. Once a data breach has occurred, companies face difficult decisions over what to do next. Do they notify the affected individuals? Are they are required to or not? And, if they do notify, in what way should they provide the notice? These decisions are made even more difficult because state laws governing notification requirements are each somewhat unique.[93]

First, while the effects of a company hacking are far-reaching and often span across numerous states and even countries, a micro-oriented, local response is the more efficient way to deal with data breaches and is therefore properly in the realm of the states.[94] Indeed, hacking and data breaches are ubiquitous.[95] With thousands of breaches occurring every day, with technology progressing far faster than any safeguard can be set in

whereas most data breaches are not. It is important to understand what makes these situations distinguishable.

[90] 794 F.3d at 697.

[91] *Id*. at 693–94.

[92] Jeffrey S. Sutton, *A Review of Richard A. Posner, How Judges Think*, 108 MICH. L. REV. 859, 863 (2010) (explaining that "'narrow opinions' are more apt to produce unanimity; unanimity limits rather than aggravates the risk of 'political' judging by accommodating more rather than fewer perspectives; unanimity enhances the Court's credibility when it makes difficult decisions about issues that Americans care deeply about; and while narrow decision making assuredly buys time, that time may be well spent in allowing more compelling answers to a difficult problem to emerge").

[93] THOMAS, *supra* note 6. ("In the United States, most states and the District of Columbia have enacted data breach notification laws that require companies that own or license personal information to notify affected individuals in the event the company discovers or becomes aware of a breach of security involving certain types of information.").

[94] *See* Sara A. Needles, *The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law*, 88 N.C. L. REV. 267, 288 (2009) (arguing for a state-based approach instead of a federal approach because state laws are tailored to protect specific interests and state laws are already supplemented by Federal, industry-specific laws).

[95] Jose Pagliery, *The Cybercrime Economy: Half of American Adults Hacked this Year*, CNN TECH (May 28, 2014, 9:25 AM), http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/index.html [https://perma.cc/39XY-ZT6S]. In 2014 alone, 432 million accounts were hacked as well as 110 million Americans. *Id.*

place, and with seemingly every entity being vulnerable,[96] the federal government is simply too big of an entity to handle such a hurricane of issues.[97] In a situation such as this, it is far better to have fifty different states, each with its own tailored procedure and separate funding, be responsible for combating data breaches and determining best practices for informing the public.[98]

Second, each state and its attorney general is highly incentivized to see that its citizens are not falling victim to hackings.[99] Simply put, state notification laws can be amended and specifically crafted to benefit the

---

[96] Andy Greenberg, *The NSA Official Has A Rogue Contractor Problem*, WIRED (Oct. 5, 2017, 5:43 PM), https://www.wired.com/story/nsa-contractors-hacking-tools/ [https://perma.cc/J6AV-8AGT]. Even the NSA was hacked. *Id.* How much confidence should consumers really have with the average store (e.g. Target, Walmart, etc.)?

[97] *See* Needles, *supra* note 94, at 308 ("A federal law that aims to address the complex, multivariable definition of personally identifiable information, let alone the manner in which companies must respond to breaches, would not be nimble enough to remain relevant in a rapidly changing industry.").

[98] *See Cybersecurity and Data Privacy Outlook and Review: 2016*, GIBSON DUNN (Jan. 28, 2016), https://www.gibsondunn.com/cybersecurity-and-data-privacy-outlook-and-review-2016/ [https://perma.cc/Q8UQ-Z8ZQ] (explaining the criticism of the proposed Data Security and Breach Notification Act by privacy activists on the position that the bill would preempt state laws that are more effective in protecting consumer privacy and because the notification requirements would be "triggered only if the company decides there is a risk of financial harm, which, in [the] critics' view, gives companies too much discretion and would lead to incidents being underreported.").

[99] *Id.* ("2015 saw many states updating their data breach notification laws . . . ."). Indeed, even the National Association of Attorneys General (NAAG) supports state autonomy over federal control. They have recently sent a letter to Congress urging Congress to keep states in control of data breach legislation enforcement. *See also Federal Data Breach Legislation Should Not Preempt States*, NAAG, http://www.naag.org/naag/media/naag-news/federal-data-breach-legislation-should-not-preempt-states1.php [https://perma.cc/URS2-T2D3]. The NAAG's primary concern is that a majority of current federal bills that pertain to data breach notification and security preempt the states. *Id.* The letter, signed by 47 state and territorial attorney generals, explain that preempting state law—and thereby giving federal government more power—would in fact make consumers less protected. *Id.* Unlike the federal government, the "States are on the front lines in helping consumers deal with the repercussions of a data breach" and are therefore can take a more tailored approach. *Id.* This approach stems from the fact that "attorneys general regularly investigate the causes of data breaches to determine whether data collectors . . . used reasonable data security practices and notified consumers . . . according to the requirements of state law." *Id.* In addition to these reasons, the States have already "adopt[ed] data breach notification laws [since] 2003, and some have since required data collectors experiencing breaches to directly notify the attorney general in order to respond more quickly to concerned consumers[,]" which in turns provides for a more expedited and targeted response. *Id.* Finally, the letter from NAAG makes several important final notes: (1) that it is imperative that the States continue to "enforce breach notification requirements under their own state laws;" (2) with any federal law being passed, the states should still be allotted sufficient "flexibility to adapt their . . . laws to respond to changes in technology and data collection[;]" and (3) the power to place "requirements on data collectors that go beyond those required at the federal level[,]" should stay within the states. *Id.* In sum, there is a strong consensus that federal law operates best when innovative state law and enforcement supplement it. *Id.*

consumer by forcing companies to provide better means of relief and stronger safeguards against such hacks.[100]

Third, while every state has its own financial issues, on average, state-wide data breach notification laws and procedures backed by state funding would fare better (again, think micro not macro).[101] The federal government simply does not have enough funding to cover the series of hacking incidents that are springing up every day, each its own isolated and unique, festering problem.[102] The states, however, have less projects that need financial support than the federal government; and therefore, the states are in a better position to provide relief after a damaging hack.[103]

Finally, states are better suited to enact laws that take preventative measures to counter data breaches. Preventative measures are critical for safeguarding consumers from data breaches. Often, companies that have been targeted by hackers and that have suffered data breaches are able to avoid paying damages because they never promised to safeguard the consumers' information.[104] However, this is wrong and unfair. State laws should require companies to take affirmative steps to ensure that their consumers' information is protected.

Implementing an affirmative step requirement on companies and businesses to protect consumer information would not only act as a

---

[100] *See* Needles, *supra* note 94, at 302 ("Businesses have a market-based incentive to create and abide by strong breach notification policies.").

[101] *See* John S. Kiernan, *2017's Most & Least Federally Dependent States*, WALLETHUB (Mar. 19, 2019), https://wallethub.com/edu/states-most-least-dependent-on-the-federal-government/2700/ [https://perma.cc/V7EU-TCZN].

[102] *See USA Debt Clock – How Much Is The US National Debt?*, COMMODITY, https://www.nationaldebtclocks.org/debtclock/unitedstates [https://perma.cc/E8JP-2WAV]. *But see* Annie Lowrey, *Are States Really More Efficient Than the Federal Government?*, ATLANTIC (Oct. 2, 2017), https://www.theatlantic.com/business/archive/2017/10/graham-cassidy-states-federal-efficiency/541599/ [https://perma.cc/6BUN-FL48] (noting that "turning programs over to the states tends to result in the 50 capitals pursuing varying policy priorities and achieving disparate policy outcomes—not in a sleeker, more efficient government"). However, given the strong public policy interest in protecting consumers from harm, any likely disparities in how the states approach their data breach notification responses would only vary in severity of punishment—not necessarily in effectiveness of curing harm.

[103] However, none of this is to say that the federal government is to sit on its hands; the opposite, rather, is needed in that the federal government should provide more funding against cyber-related attacks, should create more hacking-specific task forces, and should make it clear that cyber-attacks are the biggest threat to national security that this country has ever seen.

[104] Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 COMPETITION: J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL. 229, 231 (2015) ("Historically, courts have refused to construe generic statements on company websites or promotional materials—that consumer data was safe or protected by certain security measures, such as firewalls or encryption—as express contractual obligations, or to imply contracts from such statements or the customer relationship at large."); *See e.g., In re* Zappos.com, Inc., No. 3:12-cv-00325-RCJ-VPC, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013) ("Plaintiffs allege that [defendant] breached a contract to safeguard their data. But there is no allegation of any express or implied contract.").

deterrence for hackers, it would incentivize businesses to create stronger cyber-walls and develop a better relationship with consumers and government agencies.[105] On a state level, the local governments would be in a much better position to determine the proper affirmative step requirements and would also be better suited for understanding what would incentivize local businesses.[106]

CONCLUSION

This note provided an overview of a serious and uncharted area of the law and the everyday lives of Americans. It briefly discussed hacking and the various methods used by hackers. It then discussed two key cases, *Clapper* and *Remijas*, and their respective facts and holdings. Finally, this note proceeded to analyze the holdings of these cases and the discussion between state and federal data breach laws. One thing is certain in the area of the law where people's data is mined and sold like gold, where privacy

[105] While it could be argued that this would not be economically feasible for many business, especially smaller businesses, this type of implementation would have to operate on a case-by-case basis. As such, this is why state-wide data breach notification laws are better suited for this. Additionally, these requirements should come with both a reward for meeting the requirements and a punishment for failing to do so. Meaning, if a business or company meets the affirmative steps to ensure consumer information safety, in the event of a data breach, they should be given some lenity—or even a safeguard against certain types of damage. On the other hand, if these steps are not taken, the business should suffer stringent consequences such as paying extra fines, paying for certain number of years of credit monitoring, and perhaps even being held *per se* liable for certain damages depending on the severity of the breach. *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/5C27-8J7Z] (arguing that "incentives for companies to protect data should skew toward prevention, rather than self-flagellating disclosures. Disclosure after the fact only helps the legal and compliance industries that have cropped up in the wake of recent breaches"). While I agree with O'Connor on this point, I cannot agree with a majority of her article—especially the arguments for a single comprehensive federal law as opposed to the "patchwork" of state laws. It is easy to peg the various state laws as a "patchwork" since they are not in uniformity. But to do so, and to argue that because they lack a uniformity that they are therefore inferior to a single, uniform federal law, is, at the very root, taking this debate back to the 1790's between Alexander Hamilton and Thomas Jefferson. The Federalists, led by Alexander Hamilton, advocated for a strong central government; whereas Thomas Jefferson and the Republicans, or Democratic-Republicans vied for strong states' rights. *See American History From Revolution to Reconstruction and Beyond: Hamilton vs. Jefferson*, UNIVERSITY OF GRONINGEN, http://www.let.rug.nl/usa/outlines/history-2005/the-formation-of-a-national-government/hamilton-vs-jefferson.php [https://perma.cc/KBZ2-NPSN]. With history in mind, the debate has not changed in substance, but, perhaps only in form.

[106] Again, while this argument may begin to look like the classic Federalist versus Republican debate, this situation necessitates a fine-tuned and tailored approach that only the states can bring on an individual basis.

is seemingly a forgotten principle,[107] and where nothing can be hidden from the public eye: change is necessary.

[107] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 220 (1890) ("Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?").